AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-0108

Authentifizierungs-Bypass im PAN-OS Management-Interface.

Ein nicht authentifizierter Angreifer mit Netzzugang zum PAN-OS-Management-Interface kann die Anmeldung umgehen und bestimmte PHP-Skripte aufrufen – ohne gültige Zugangsdaten. Allein ermöglicht das kein Fernausführen von Code, wohl aber das Auslesen von Konfiguration und sensiblen Daten. In der Praxis wird die Lücke aktiv und in Verkettung mit CVE-2025-0111 und CVE-2024-9474 ausgenutzt, um vollen Gerätezugriff zu erlangen.

> **Geschäftsrisiko:** unbefugter Zugriff auf die Firewall-Verwaltung – mit Potenzial für den Abfluss von Konfigurations- und Zugangsdaten, Manipulation der Sicherheitsrichtlinien und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

8,8 / 10

HOCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:A/AU:N/R:U/V:C/RE:M/U:Red`
– aus dem Netz, ohne Rechte, ohne Zutun – hohe Wirkung auf die Vertraulichkeit, geringe auf die Integrität des Firewall-Managements. Das NVD bewertet dieselbe Lücke nach CVSS 3.1 sogar mit 9,1 (kritisch).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Februar 2025	PAN-OS 10.1 · 10.2 · 11.1 · 11.2 (Management-Web-Interface)	Sofort

Das Wichtigste in 60 Sekunden.

8,8 · HOCH
CVSS 4.0 · NVD 3.1: 9,1

Auth-Bypass
Management-Web-Interface

Aktiv
ausgenutzt · CISA KEV · verkettet

Cloud NGFW
& Prisma Access nicht betroffen

Die Ursache: Das PAN-OS-Management-Interface prüft bei bestimmten Anfragen nicht zuverlässig, ob der Aufrufer angemeldet ist (CWE-306, fehlende Authentifizierung für eine kritische Funktion). Ursache ist eine Diskrepanz, wie die vorgelagerte Webserver-Komponente und die dahinterliegende Anwendung Pfade normalisieren – dadurch lassen sich geschützte PHP-Skripte ohne gültige Sitzung erreichen. Ein Aufruf ermöglicht kein direktes Code-Ausführen, aber den Zugriff auf schützenswerte Funktionen und Daten – und dient als Einstieg für die Verkettung mit weiteren Schwachstellen.

ANGRIFFSKETTE

01	02	03	04
Interface exponiert – das Management-Web-Interface ist aus dem Netz erreichbar	**Anmeldung umgehen** – ohne Zugangsdaten geschützte PHP-Skripte aufrufen	**Verkettung** – mit `CVE-2025-0111` (Datei-Lesen) und `CVE-2024-9474` (Rechteausweitung) kombinieren	**Zugriff** – Konfiguration und Zugangsdaten auslesen bis zur vollständigen Geräteübernahme

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.1	`< 10.1.14-h9`	`10.1.14-h9`
10.2	`< 10.2.13-h3 (mehrere h-Zweige)`	`10.2.13-h3`
11.1	`< 11.1.6-h1 (mehrere h-Zweige)`	`11.1.6-h1`
11.2	`< 11.2.5 / 11.2.4-h4`	`11.2.5`
11.0 · 10.0 · 9.x (EoL)	als betroffen anzunehmen	auf unterstützten Zweig migrieren
Cloud NGFW · Prisma Access	nicht betroffen	—

Angreifbar ist ausschließlich das **Management-Web-Interface**. Innerhalb der 10.2- und 11.1-Zweige existieren mehrere Hotfix-Stände – die exakte Fixversion gegen das Hersteller-Advisory des eigenen Zweigs abgleichen. End-of-Life-Versionen erhalten keine Fixes und sind zu migrieren.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Firewall-Verwaltung kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

12.02.2025
kurz darauf

18.02.2025
CISA KEV · Frist 11.03.2025

Seither

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff einschränken vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Management-Zugriff einschränken	Patch einspielen	Threat Hunting / Log-Abgleich

01 Exposition feststellen

Prüfen, ob das Management-Web-Interface aus nicht vertrauenswürdigen Netzen erreichbar ist – insbesondere aus dem Internet. Nur exponierte oder von unvertrauten Quellen erreichbare Interfaces sind angreifbar.

02 Sofort mitigieren (vor dem Patch)

Zugriff auf das Management-Interface auf vertrauenswürdige interne IP-Adressen beschränken (Best Practice von Palo Alto: Management getrennt vom Datenverkehr, nie direkt aus dem Internet erreichbar). Zusätzlich die Threat-Prevention-Signaturen aktivieren:

```
Threat IDs 510000 & 510001 (Applications and Threats 8943+)
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.1.14-h9` · `10.2.13-h3` · `11.1.6-h1` · `11.2.5` bzw. der passende h-Fix). End-of-Life-Zweige (11.0, 10.0, 9.x) erhalten keinen Fix und sind auf einen unterstützten Zweig zu migrieren.

04 Kompromittierung ausschließen

Management-Zugriffs- und System-Logs auf unauthentifizierte Aufrufe von PHP-Skripten sowie auf Anzeichen der Verkettung mit CVE-2025-0111 / CVE-2024-9474 durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Management-Interface dauerhaft aus öffentlichen Netzen herausnehmen, dedizierte Management-Netze/Jump-Hosts nutzen und Content-Updates zeitnah einspielen, damit IPS-Signaturen wirken.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFSFLÄCHE

Unauthentifizierte Zugriffe auf das `Management-Web-Interface` (HTTPS-GUI) und geschützte PHP-Skripte

VERKETTUNG

Nachgelagerte Ausnutzung von `CVE-2025-0111` (Datei-Lesen) und `CVE-2024-9474` (Rechteausweitung)

THREAT-IDS (IPS)

Palo Alto Threat Prevention `510000` · `510001` (Content 8943+)

Zur Einordnung: Die beobachteten Angreifer-Quell-IPs sind flüchtig und wechseln laufend (u. a. über GreyNoise nachverfolgbar) – daher hier bewusst keine statische Liste. Maßgeblich ist die Analyse Ihrer eigenen Management-Zugriffs- und System-Logs auf unauthentifizierte Aufrufe.

Wichtig: Erfolgreiche Zugriffe erscheinen als vermeintlich reguläre Aufrufe des Management-Interfaces – ohne Alarm. Ohne Auswertung der Zugriffs- und System-Logs bleibt ein bereits erfolgter Bypass unsichtbar; ein direkt aus dem Internet erreichbares Management-Interface ist das eigentliche Risiko.

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Unauthentifizierte Zugriffe auf das Management-Interface und anomale GUI-Sitzungen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte PAN-OS-Management-Interfaces über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre PAN-OS-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Management-Zugriff heute einschränken, Patch innerhalb weniger Tage einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Grundsätzlich entscheiden, dass Management-Interfaces nie direkt aus dem Internet erreichbar sind.

Ihr Part · unser Part. Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2025-0108 und dem PAN-OS-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: Palo Alto Networks Security Advisory CVE-2025-0108 · NVD (CVSS 3.1 9,1 / CVSS 4.0 8,8, CWE-306) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 18.02.2025, Frist 11.03.2025). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.